INTERNAL/EXTERNAL AUDITS CHAPTER 8

(FILE NAME ON DISK # 1 = S1C8.WPD)

The FFIEC member agencies believe that a strong internal auditing function combined with a well-planned external auditing program substantially increase the probability that an institution will detect potentially serious technology-related problems. A strong internal auditing function helps to assure a proper control environment and promotes accuracy and efficiency in an institution's operations. An external auditing program complements this function by providing an objective outside view of the institution's bank's operations.

Adequate internal controls should be structured to assure senior management that:

- Records are being processed accurately and in a safe and sound manner.
- Accounting data is reliable.
- Operating procedures are efficient and effective.
- Procedures are in effect to assure continuity of services.
- High risk conditions, functions, and activities are identified and effectively monitored.
- There is proper adherence to management standards and policies, applicable laws and regulations, regulatory statements of policy, and other guidelines.

An independent audit must be performed to ensure that these controls are maintained effectively.

The institution's board of directors must provide for an adequate independent audit. This audit may be performed by the board of directors or one of its committees or it may be delegated to other qualified persons. The board may either:

- Provide an internal audit function capable of evaluating information systems controls.
- Engage outside consultants or auditors to perform the audit.
- Use a combination of both methods to ensure that the information systems area has received adequate audit coverage.

Regardless of the method used, the auditor should report and be accountable to the board of directors or its designated committee. This accountability precludes the auditor from certain relationships that may compromise audit independence.

This section provides a general discussion of the information systems audit function and objectives and methods that may be used to provide appropriate audit coverage. Since information systems is an ever-changing field, this section should be used as a guide in understanding the purpose of a sound information systems audit program, regardless of how technological innovations affect its operations.

EXTERNAL AUDIT POLICY GUIDANCE

Financial institutions of all sizes are encouraged to have both internal and external audit coverage of IS activities. All financial institutions should develop and maintain an appropriate level of external auditing activities. The Federal Deposit Insurance Corporation issued two policy statements primarily targeting smaller community banks in 1988 and 1990 respectively. They covered in some detail guidance addressing both independent external auditing programs and external auditing procedures. These two policy statements, dated December 28, 1988, and January 22, 1990, can be referenced in their entirety in the Chapter 26 of this Handbook. The 1988 policy acts as an appropriate reference for all banks. It specifically encourages state nonmember banks to adopt an external auditing program that includes an annual audit of financial statements by an independent public accountant. The 1990 policy statement provides external audit procedures to be included in a comprehensive external audit program. These guidelines also include basic audit procedures for IS activities.

SELECTING THE AUDIT STRUCTURE

The institution should have written guidelines for the conduct of the information systems audit. The selection of auditor(s) should be approved by the board of directors.

Although the board may delegate the audit performance, it must ensure their quality. The board must periodically review and approve:

- The qualifications and independence of the audit function.
- The scope and frequency of the audit, based on an assessment of risk.
- The current year's audit schedule.
- Reports comparing actual audit work performed versus the approved audit schedule.
- The techniques used in performing the audit.
- The overall condition of the organization's information systems controls and operations.
- Management's actions to resolve material weaknesses cited in audit reports.

Information systems audit coverage may be provided by an internal audit staff, external auditors, or a combination of both. Audit personnel must have sufficient information systems expertise to perform data processing audits. This expertise should be commensurate with the scope and sophistication of the institution's data processing environment. If the internal expertise is inadequate, external sources, such as management consultants, CPA firms, qualified professionals or correspondent banks should be contacted to supplement or perform, the information systems audit function.

Financial institutions increasingly receive outside information systems services from wholly owned subsidiaries, affiliates, bank service corporations, facilities management groups, or independent service companies. The contractual agreement between the service provider and the institution must define audit responsibilities. The board of directors should determine the type of audit that is best for the institution and consider various approaches that include:

- *Audits by the servicer's internal auditor.* To rely on this approach, the board of directors must be assured of the independence, competency, and scope of the audit and it must evaluate the audit results. All exceptions noted in the audit should receive follow-up review to ensure proper resolution. Integration of the serviced institution's internal audit program with that of the servicer should be considered.
- *Audits by an institution's internal or external auditor.* Audits completed by the internal or external auditors should be complimentary in scope and quality. They will be linked directly to its information systems control features or be part of its overall audit. Audit personnel should possess sufficient information systems expertise to conduct an effective audit.
- *Audits through a third-party review.* This method provides for a qualified auditor, who is independent of both the servicer and the serviced institution(s), to review the servicer's operation. The scope of the review is determined normally by the third-party auditor and should be detailed enough to satisfy the audit objectives of the serviced institution and servicer. Generally, the review would complement the financial institution's internal audit program. (Further discussion of third-party reviews may be found in later in this chapter.)
- *Cooperative audits.* If many financial institutions receive services from a common servicer, they may arrange for one audit that would satisfy the requirements of all the participating serviced institutions, i.e., user group. These audits may be performed by internal or external audit personnel. This method should incorporate the following guidelines:

- All serviced financial institutions should be invited to participate in the audit arrangements.
- Costs of the audit should be allocated fairly among all participants.
- All participating auditors should be qualified.
- The audit should be supervised by a committee of officers or directors representing the participating institutions.
- The audit scope and procedures should be identified and agreed to by all participants.
- The auditors' written charter should identify clearly reporting responsibilities, report distribution, and follow-up guidelines.

Whatever method is used, documentation of the scope and audit findings should be maintained at the serviced institution. Any follow-up review or review by the board or senior management, together with remedial action initiated to correct disclosed deficiencies, should be similarly documented and kept on file.

ROLE OF THE INTERNAL AUDITOR

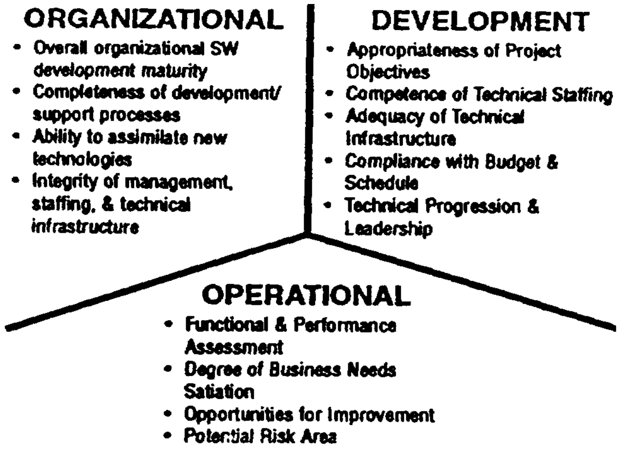
The internal audit includes an independent appraisal of information systems operations for the board of directors. Auditors evaluate the day-to-day information systems controls to ascertain whether transactions are recorded and processed in compliance with acceptable accounting methods and standards set forth by the board of directors and senior management. Auditors also perform operational audits, including information systems development auditing, to assure management that policies and procedures are effective as designed and followed by employees. (Refer to Figure 8.1.)

Auditors should furnish management with analyses, appraisals, recommendations, and other comments on activities reviewed. These comments will assist management in using its resources more effectively. The internal auditor is concerned with all phases of business activity and must look beyond accounting and financial records to obtain a full understanding of the operations under review.

The internal auditor should:

- Review, appraise, and report on the soundness,adequacy and application of accounting, financial and other operating controls.
- Promote effective control at a reasonable cost (for example, by suggesting certain controls and stressing their importance).
- Determine the extent of compliance with established policies, plans, procedures, and laws.
- Determine the extent to that assets are accounted for and safeguarded from loss.
- Assess the reliability of and the timely processing of management data developed within the organization.
- Track progress in complying with regulatory requirements and recommendations.
- Recommend alternatives to correct control deficiencies.

Figure 8.1
The Focus of the Audit May Shift


ORGANIZATIONAL
• Overall organizational SW development maturity
• Completeness of development/ support processes
• Ability to assimilate new technologies
• Integrity of management, staffing, & technical infrastructure
DEVELOPMENT
• Appropriateness of Project Objectives
• Competence of Technical Staffing
• Adequacy of Technical Infrastructure
• Compliance with Budget & Schedule
• Technical Progression & Leadership
OPERATIONAL
• Functional & Performance Assessment
• Degree of Business Needs Satiation
• Opportunities for Improvement
• Potential Risk Area

With Permission M. Zola Rapid Systems Solutions, Inc.

The institution's board of directors should adopt a charter or issue a policy statement clearly establishing the responsibilities of internal auditors.

The charter should identify the purpose, responsibilities, and authority of the audit department. It should state clearly the auditor's right to access all records, policies, plans, procedures, and properties and to question personnel about the matters under review. The audit charter should include a statement of audit independence and support from the board of directors.

INDEPENDENCE AND STAFFING OF INTERNAL IS AUDIT

Competence

The overall competence level required for an internal information systems audit function depends upon the size and complexity of its operations and the responsibly delegated to the auditor. In some institutions, the internal audit is performed by a person or group that has no other responsibilities except information systems auditing. In other cases, particularly in smaller institutions, audit responsibility is assigned to an officer or employee designated as a part-time auditor. Such an auditor may plan and perform all audits personally or may use staff borrowed from other departments. An information systems auditor on a small staff should be a skilled generalist. Always, the information systems auditor should possess expertise commensurate with the sophistication of the system(s) audited.

An internal information systems auditor should have:

- A sound knowledge of bank accounting practices and recordkeeping requirements.
- A firm understanding of management concepts and practices and the fundamental principles of internal control.
- The ability to direct, plan, schedule, and supervise specific audit functions.
- The ability to investigate thoroughly and to document this work.
- The ability to communicate tactfully (orally and in writing) with those subject to the audit and to senior management.
- The ability to derive, summarize, and report criticisms effectively and constructively.
- A general understanding of systems design and project management concepts.
- A general knowledge of operating systems, automated applications, methods of storing and retrieving data files, i.e., programming, file organization and documentation, direct access storage devices, and controls customarily used in information systems.
- Knowledge of, and expertise in, information systems auditing concepts and techniques.
- The ability to identify general installation security measures and work flow, including risk analysis and threat assessment.
- A working knowledge of data processing technology.

A financial institution's hiring and training practices are important in considering the qualifications of information systems auditors. The auditor's education and experience should be consistent with job responsibilities. Although information systems auditors do not have to be computer experts, they should be able to recognize how use of a computer can enhance the audit. As the information system becomes more sophisticated or as more complex technologies evolve, the auditor must be given additional training. In the interim, outside technical experts or consultants could be engaged to assist with more complex audits.

Since the computer environment is evolving as new technologies are introduced, audit management should provide a program of continuing education for auditors. Available sources of technical and information systems audit training include:

- Participation in conferences and seminars sponsored by banking and professional associations.
- Courses sponsored by hardware or software vendors (audit and application), colleges, universities, and local technical schools.
- Self-study and programmed learning (technical periodicals, video instructional programs, etc.).
- Monitored on-the-job training, including in-house cross training.

In institutions where the information systems auditor reports to an audit manager, the manager should be familiar with pertinent technical concepts. This will enable him/her to guide information systems audit work, establish an overall plan for audit coverage, and schedule and coordinate this plan with the general internal audit program. The manager should also coordinate the internal audit department activities with those of regulatory authorities and external auditors.

The overall measure of an auditor's competence is based upon the quality of the work, the ability to communicate work results, and effectiveness in obtaining correction of cited deficiencies.

Independence

The ability of the internal audit function to achieve desired objectives depends largely on the independence of audit personnel. Generally, the location of the auditor administratively within the organization, the reporting authority for audit results, and the auditor's responsibilities indicate the degree of their independence.

Internal auditors should be functionally directed by the board of directors or the audit committee. The board must ensure that the audit department does not participate in activities that may compromise its independence. These activities may include preparing records, developing procedures, or performing other operational duties normally reviewed by auditors.

However, auditors should make recommendations to management about procedures that affect information systems controls. In this regard, the audit department should review the control aspects of any new application throughout its development. This should ensure that proper controls and audit trails are included in the application so that an effective audit review can be performed more easily.

The auditor's independence is also determined by analyzing his/her reporting process, findings, and recommendations. For an effective program, the auditor should be given the authority: (1) to obtain all records necessary to conduct the audit, and (2) to require management to respond formally to adverse audit findings and to take appropriate corrective action.

By reporting audit results directly to the board of directors, the auditor assists it in fulfilling its audit responsibilities. Internal auditors should be able to discuss their findings and recommendations periodically with directors who are not officers of the institution. If officers or inside directors attend those meetings, their participation should be limited to encourage candid discussion.

To ensure the auditor's continued independence, the auditors should be informed of the standards they are required to meet in their behavior and work.

INTERNAL AUDIT RISK METHODOLOGY

A proper level of audit coverage of the information systems environment requires an effective audit risk analysis methodology. This analytical methodology should provide the internal auditor and the board with objective information to prioritize the allocation of audit (internal and/or external) resources properly. This should ensure:

- More timely audit reporting on high risk conditions in operating units.
- Enterprise-wide risk control functions (e.g., contingency planning, and corporate information security).
- Project activities related to procurement and implementation of new systems.

At a minimum, the IS audit program should provide:

- Identification of audit units, including systems development projects and enterprise-wide risk control functions, based on understandings of IS risk exposures (e.g., that threaten data integrity, financial condition, financial performance, continuity of operations, regulatory compliance, and customer service).

- Maintenance of the universe of audit responsibility including areas to be audited.

- Maintenance of IS risk-based audit coverage plan (e.g., differentiates high, medium, and low risk audits) that includes explanation of audit frequency and resource requirements.

- Detailed analysis and support for a risk-based annual audit schedule approved by the board of directors.

The auditor must work closely with management and the board to obtain proper understandings and perspective on the information risk exposures.

Frequently, integrated audits (i.e., coordination of financial audits and IS audits) address traditional financial audit test objectives, but sometime fall short in operational auditing. For example, a financial audit would generally not cover certain business controls that are normally inspected in an operational audit of the contingency planning process. These business controls include the mission statement for enterprise-wide contingency planning, the charter statement delineating the scope of management responsibilities, contingency plan performance objectives and criteria, and all other operational requirements for the computer center(s), networking/telecommunications, and business resumption recovery.

INTERNAL AUDIT MANUAL

The internal audit manual should define the role of the audit department within the organization and describe the overall audit scope and objectives. The manual often written by the internal audit department should reflect the needs of the institution and the philosophies of the audit committee or auditor. The procedures should establish appropriate guidelines for auditing information systems operations, applications, and user department controls. An internal audit manual is a prerequisite for an effective audit program.

The manual should be reviewed and approved formally by the board of directors. The board must determine whether adherence to its standards and procedures will result in a comprehensive audit. Once approved, the manual will provide the audit department with uniform standards for performance and serve as a valuable training aid for audit personnel. In addition, it will assist the board in evaluating audit work performed and the competence of audit management.

The manual should contain written policies, standards, and procedures for the audit department. These include:

- Administrative and general department personnel policies, including those relating to goals and objectives, hiring, training, performance reviews, and job descriptions.
- Organizational and reporting structure.
- Areas or functions to be audited.
- Audit frequency and scheduling guidelines, including a description of the methodology used for assessing risk in the areas to be audited.
- Detailed procedures for the audit of all significant applications and functions within automated data processing.
- Guidelines for microcomputer audits.
- Guidelines for audit involvement and review of a system's development life cycle.
- Standards for audit workpapers and reports, e.g., content, format, filing and distribution, and report follow-up.
- Standards and procedures for audit software, including its development, purchase, documentation, use, maintenance, and control.

The manual must be modified periodically to reflect appropriate changes in audit procedures caused by a change in scope or by increased sophistication within the audit department, the data center, or end user departments. If those changes affect the audit program significantly, they should be reviewed and approved by the board of directors.

PLANNING, ORGANIZING, AND SUPERVISING AN IS AUDIT

Planning

The effectiveness of any internal audit program depends upon the soundness of audit practices and proper planning. The more precisely the audit objectives are identified, the more likely supporting procedures will be appropriate and carried out effectively. The planning function includes:

- Setting objectives, formulating procedures, and preparing a budget.
- Obtaining sufficient resources for accomplishing the organization's audit objectives.
- Compiling a list of reports, information, and other aids to be requested from the audited area.
- Assigning responsibilities to accomplish the objectives within budget restrictions.
- Reappraising objectives, procedures, and budgets to meet changing conditions.

For example, the objectives of the information systems applications audit can be accomplished by dividing the task into basic steps. Each step should have a defined purpose and carefully detailed procedures for its completion. Those procedures should give the auditor sufficient guidance to perform the audit yet allow for discretion. As each audit step is performed, the auditor should be able to identify areas that require more extensive coverage.

Organizing

Once the audit plan is developed, the auditor must organize staff and materials to accomplish it. Organization of the audit plan includes establishing a structure and a system designed to:

- Achieve the objectives.
- Assign responsibilities for carrying out the plan.
- Maintain continuity of organization and responsibility.
- Reappraise the structure and system periodically to ensure their continued effectiveness.

Supervising

Supervision is directing, coordinating, and regulating the audit pursuant to planning requirements and to accomplishing stated objectives. The degree of supervision required depends upon the competence of the persons performing the audit and the sophistication and risk associated with the particular area being audited. Supervision generally includes:

- Determining the scope and frequency of information systems audits.
- Establishing standards, including costs and quality of work, for the audit department.
- Ensuring compliance with audit standards by reviewing and signing off on completed workpapers and audit reports.
- Maintaining the audit standards by monitoring procedures, obtaining feedback, and making appropriate adjustments to meet changing conditions.
- Training personnel to comply with the standards.
- Following-up to ensure that report responses are received promptly and address all points as required under the audit program.

Scope and Frequency of Information Systems Audit Coverage

The scope of the procedures and frequency of internal auditing must be sufficient to accomplish the audit objectives. Covered areas are:

- *Compliance review* – Adherence to established policies, standards, and procedures.
- *Quality review* – The quality of formal policies, standards, and procedures, and of management, efficiency of operations, and the adequacy of procedures and controls.
- *Integrity review* – Fraud detection/deterrence, application program and operating system integrity, application system design and implementation, and monitoring employee activities and access levels.

Within these categories, such functions as reconcilements, data entry control, computer operations, systems development, program change, data communications, output distribution, and user department data processing controls will be reviewed. The frequency of audits should be based on the risk associated with each area of audit interest. Among the factors that auditors should consider in assessing risk are:

- The nature of the specific operation and related assets and liabilities.
- The existence of appropriate policies and internal control standards and procedures.
- The effectiveness of supervision, including policies, operating procedures, and internal controls.
- The potential effect of errors or irregularities associated with the specific operation.
- The sensitivity of the information involved.
- The results of past reviews and the current state of identified problem areas.

All areas of information systems operations should be reviewed within an approved audit cycle or annual review. Audit frequency and scope should be associated directly with the inherent risk in an operation or application function. As such, some activities will be reviewed more frequently than others. The board, or its audit committee, should approve the audit schedule each year. It should be apprised of significant deviations to the audit schedule resulting from budget constraints, staff turnover, or other contingencies. If the audit schedule is not completed within the expected cycle, the reasons should be documented and reported to the audit committee. Major adjustments to the schedule should be approved by the committee or the board.

AUDIT PROCEDURES

Information systems audit procedures will vary depending upon the philosophy and technical expertise of the audit department and the sophistication of the data center and end-user systems. However, to achieve effective coverage, the audit program and expertise must be consistent with the level of data processing activities being reviewed. The audit procedures may include manual testing processes or computer-assisted audit programs. Usually, a combination of manual and computer-assisted audit techniques will be used.

Internal auditors may choose techniques to test records that do not use the computer. For these methods to be effective, the control environment in that data processing is performed must be considered. Such methods may include comparing a representative sample of records with source documents or verifying them independently through direct confirmation. The results of these procedures should be reconciled in the same manner as in an audit of manually prepared records.

When computer audit programs are used, internal information systems auditors should perform application reviews, compliance and substantive tests, and record evaluation, to verify the adequacy of internal controls. Discussions of the implementation of each approach follows:

Application Review

- Use questionnaire.
- Interview personnel in data processing.
- Develop a general system description.
- Review major controls of user and data processing departments.
- Review programmed controls for each application essential to the audit.

Compliance Tests

- Examine evidence relating to controls, e.g., error listings, batch control records.
- Use printouts to trace items in output to source documents, source documents to reports, report totals to controls, etc.
- Check sample transactions for correct processing.
- Assess the adequacy of test data to determine that testing is comprehensive.
- Test accuracy of summary accounts (foot, crossfoot, etc).

- Test samples of detail items by confirmations, reasonableness tests, etc.

Records Evaluation

- Reconcile user control totals to processing activity and computer report totals to general ledger figures.
- Determine that user department, data processing department, and programmed controls function are documented.

Using Computer-Assisted Audit Techniques

Auditors should strive to use the computer in performing audits. The computer can improve audit coverage by reducing the cost of testing and sampling procedures that otherwise would be performed manually. It also can better check data integrity by testing the logical processing of data "through" the system rather than relying only on validations of input and output controls.

Audit software is available to:

- Test footings and computations to verify the accuracy of information systems outputs.
- Test records for completeness, logical consistency, validity of conditions, and reasonableness of amounts.
- Summarize and analyze operating efficiency from job accounting data.
- Test input and output data and controls for authorized processing.
- Select and print data by using statistical sampling techniques for confirmations, etc.
- Simulate independently the processing of transactions to verify the accuracy and consistency of computer programs.
- Generate audit trial balances and related reports.
- Establish an audit software library.

For audit purposes, internal auditors may use:

- Programs written by the internal programming staff or by outside programmers with audit department supervision.
- Generalized audit software, e.g., audit packages offered by CPA firms or software vendors.
- Programs written by information systems auditors.
- Programs available from equipment manufacturers and software houses to analyze machine, programmer, and operations efficiency.

Audit techniques available to test data and programs within the computer systems include:

- *Integrated test facility (ITF)* – Processing test data for a dummy department, branch or function, and comparing processing results to those predetermined. Transactions initiated by the auditor are indistinguishable from live ones and are processed at the same time as live data. Special care must be taken to partition test accounts and balances strictly to avoid understating or overstating assets. The auditor should also be aware of any local legal restrictions to the use of ITFs.
- *Parallel simulation (independent audit proof)* – Using independent software to simulate actual application processing and comparing these results with those of actual processing.
- *Audit logging* – Maintaining a computerized record of all access to a given file, including the accessing terminal and user identification.
- *Parallel operations* – Verifying the accuracy of new or revised application programs by processing production data and files, using both existing and newly developed programs. Processing results are compared to identify unexpected differences. (This technique is employed customarily by programmers and systems' analysts prior to releasing newly developed or modified applications. However, information systems auditors should be involved to ensure the thoroughness of parallel testing.)
- *Base case system evaluation* – Executing computer application programs by using test data sets developed as part of a comprehensive testing program, and verifying processing accuracy by comparing processing results with predetermined test data results. (Such testing should be performed whenever applications are modified.)

- *Embedded audit data collection* – Using audit subroutines embedded within computer applications software to screen and select for audit review input transactions and those generated within applications.

- *Transaction tagging* – Auditing an application by tagging a special code to input records as they enter a given system. The status of the live records is monitored as they flow through specific points in the application.

- *Extended records* – Adding a control field to a given record either as a special field or as a trailer record. This field or record may include data from all application programs that contributed to the processing of a transaction.

Whatever the source, audit software programs should remain under the strict control of the audit department. For this reason, all documentation, test material, source listings, source and object program modules, and all changes to such programs, must be strictly controlled. In installations using advanced software library control systems, audit object programs may be catalogued with password protection. This is acceptable if the auditors retain control over the documentation and the appropriate job control instructions necessary to retrieve and execute the object program from the libraries where it is stored. If internal control procedures within the computer system do not allow for strict audit control, audit programs should not be catalogued. Computer programs intended for audit use should be documented carefully to define their purpose and to assure their continued usefulness and reliability.

When audit software is processed, auditors must ensure the integrity of processing. Appropriate controls include:

- Maintaining physical control over the audit software, unless it is catalogued in the system and protected appropriately.

- Developing independent program controls that monitor or limit the processing of the audit software.

- Maintaining control over software specifications, documentation, and job control language.

- Controlling the integrity of files being processed and output generated.

AUDIT PARTICIPATION IN APPLICATION DEVELOPMENT/TESTING OR ACQUISITION

The development of an automated application may be a lengthy and complex process requiring a significant degree of interaction between the programming staff and user departments. To ensure that applications meet the needs of the institution, the process requires detailed developmental stages, referred to as the system development life cycle (SDLC) or system development methodology (see Chapter 12, Systems Development and Programming). As each stage of the life cycle is reached, the auditor may review internal controls and audit trails included in the application. Modification of a completed application program once in production is usually more difficult and expensive. The auditor should participate in its development to ensure that effective audit controls are incorporated from the beginning. Guidelines should be developed to facilitate the review of new applications during the design phase, so that controls can be identified for early audit review.

Earlier sections of this chapter detail the reasons why an independent objective audit function is necessary. This objectivity need not be compromised by audit input during the developmental cycle of an application. Auditors should be able to determine and recommend appropriate controls to user management. Such recommendations are not intended to be assurances that controls are absolute, but that the structure is appropriate. In this capacity, the auditor is merely a "consultant" on internal controls. Care should be exercised, however, to preclude the auditor from direct involvement in management decisions.

Once a new application system or major revision to an existing system is accepted for production processing, the information systems auditor should schedule a post-implementation review. This should occur within the first year of production. The reviews should provide for more extensive testing and auditing of the program logic, calculations, error conditions, edits, and program controls. Such testing allows for validation that the software controls function as expected. By performing the review soon after conversion to production, processing errors or other unsatisfactory conditions can be identified and resolved. This should minimize potential redesign costs or losses from processing errors or ineffective software controls.

In larger information systems facilities, divisions, such as quality assurance or change management, may have primary responsibility for post-implementation reviews. In such cases, the information systems auditor may choose not to perform a full review, but should participate nonetheless in establishing the test criteria and evaluating results.

AUDIT REPORTS AND DOCUMENTATION

The audit department should establish, within the internal audit manual, standards for audit workpapers and related communications. Workpapers should be well-organized, clearly written, and address all areas included in the audit scope.

They should contain sufficient evidence of the tasks performed and conclusions reached.

Workpaper documentation should include:

- A detailed description of the data center's current operational, administrative, and program controls and procedures.
- A copy of the audit procedures and questionnaire.
- A description of the audit scope, including the extent and results of tests performed.
- Audit supervisor's signature or initials evidencing review and approval.

Formal procedures should exist to ensure that audit findings are summarized and presented to management to communicate effectively the results of the audit. The basic guidelines are to:

- Provide information on scope and objectives.
- Summarize clearly, all significant audit findings, discuss them with line management, and report them in writing to senior management, and the board of directors.
- Discuss with the directors serious control deficiencies uncovered by audit work and any significant audit findings that remain unresolved.
- Highlight succinctly in well-written audit reports exceptions noted, potential risk exposure, and recommendations for remedial action.
- State an overall opinion of the audited function, whether there has been improvement or decline since the function was last audited, and reasons for any changes.
- Documenting in the workpapers all criticisms and observations made in audit reports.
- Have management prepare timely written responses to all audit reports.
- Follow up on exceptions to ensure that corrective action has been taken or that the board of directors has accepted the risk.

Reporting Conclusions

Completion of specific procedures in the information systems audit workprograms should lead internal auditors to conclusions that satisfies corresponding audit objectives. Conclusions must be appropriate for the audit work performed and consistent with documented findings. Auditors must use sound judgment to separate significant and insignificant findings.

Written audit reports communicate audit findings to management. The report should assist management in evaluating the quality of its information systems department and identify and suggest methods for correcting or improving any adverse conditions found. Audit reports should be timely, summarize facts, and indicate the status of previously reported exceptions. Information contained in the reports should be constructive, accurate, and presented clearly and logically, so that any negative audit report finding can more easily trigger a management decision.

Often oral discussions are crucial in presenting audit findings effectively and identifying possible solutions to uncovered problems.

AUDIT FOLLOW-UP

Prompt and effective management response to internal auditors' recommendations should be required in an information systems audit follow-up. The audit procedures should identify clearly the methods for follow-up. These procedures may include:

- Requesting a written management reply to the audit report that identifies corrective action for each deficiency.

- Subsequent testing of audits to verify resolution of deficiencies.

- Reporting to the board of directors or the audit committee on specific action taken or lack thereof.

When a critical deficiency is noted during an audit, a follow-up review should be performed to ensure that the corrective action has reduced the exposure to an acceptable level. Recommendations not accepted and deficiencies remaining should be documented in the follow-up review and reported to the board.

Without follow-up, even a comprehensive internal audit program will be less effective. Although the desirability of formal procedures is clear, the person or persons responsible for them should take the time necessary to develop effective ones. Often the internal audit manager monitors the progress of audit recommendations. Monitoring techniques must be effective, yet should not antagonize or impair the manager's relationship with operating management.

ROLE OF EXTERNAL AUDITOR

Responsibilities of external auditors should be defined clearly for the board of directors and senior management. This may be done by requiring auditors to submit engagement letters to the board prior to commencing their work. Such letters should discuss the scope of the audit, its length, and resulting reports. Often, essential audit features will be summarized in the letter and schedules attached describing specific procedures for each audited area. The engagement letter may include biographical information on personnel involved and provisions for disclosure and review of audit workpapers by the financial institution, its representatives, or regulatory examiners. In addition, the letter may specify any auditing procedures to be omitted – such as confirmation of loans or deposits – and whether the auditor is expected to render an opinion on the institution's financial statements.

External auditors may review information systems internal control procedures in their overall evaluation of internal accounting controls when auditing the institution's financial statements. CPA standards require auditor/accountants to consider the effects of information systems activity in each significant accounting application.

Generally, external auditors must review the general and application controls that affect the recording and safeguarding of assets and the integrity of the financial statements. General controls include the plan of organization and operation, documentation procedures, access to equipment and data files, and other controls affecting overall information systems operations. Application controls relate to specific information systems tasks and provide reasonable assurance that the recording, processing, and reporting of data are properly performed.

As external auditors review the system of internal accounting control, they should determine the extent that information systems are used in each significant accounting application. That should dictate the extent that information systems controls must be reviewed. The auditor selects the method and specific procedures for evaluating those controls. Most external auditing firms use a questionnaire or work- program to document their review. Generally, these questionnaires cover:

- Equipment, software, and organization.

- User department controls over data processed by information systems departments.

- Program and procedural documentation.

- Processing controls.

- Back up procedures.

- Security.

- Contingency planning.

- Internal audit function.

- Insurance.

External auditors may also make substantive audit tests independent of the institution's information systems operations.

THIRD-PARTY REVIEWS OF SERVICE CENTERS

A service center that processes work for several institutions often is subject to separate audits and examinations by external auditors, by state and federal agencies, and by internal auditors of the serviced institutions. These audits may be duplicative, creating a hardship on the center management. That burden may be minimized by arranging for a third-party audit to determine the existence and reliability of internal controls at the service center. A third-party audit, in this context, is an audit of an information systems servicer performed by auditors who are not employees of the servicer or of the serviced institutions. The third-party auditor may be engaged by the serviced institutions' management, its auditors, or the service center. The serviced institutions' auditors (internal or external) could use this third-party review to evaluate the system and controls at the service center. Normal regulatory examinations would still be performed.

The objectives, scope, and audit procedures of each third-party audit differ according to the needs of those engaging the auditor. The American Institute of Certified Public Accountants (AICPA) Statement on Auditing Standards (SAS) Number 70 provides guidance for independent auditors when auditing financial statements for an entity that uses a service organization to process its transactions. The statement also guides independent auditors who issue audit reports on service organizations for use by other auditors. Institutions using such audits to complement their own coverage should ensure that the scope satisfies their audit objectives.

Audit coverage of the service center should be as extensive as that which is appropriate for an institution's own computer center. Information systems audits should determine the adequacy of controls in all areas of the data center, including computer operations, systems and programming, and input/output controls. If serviced institutions' auditors are satisfied with the independence, competence, and specific procedures included in the third-party review, they may substitute it for their own audit.

END-USER COMPUTING AUDIT COVERAGE

Financial institution management must provide for an end-user audit function through an outside firm, an internal end-user audit program, or combination of both. The size of the institution's staff is not an acceptable excuse for the failure to meet this responsibility. Smaller institutions can develop and conduct an end-user audit function without significant expense by assigning an officer to create it and by ensuring that it is adequately documented and executed. The independence of the various audit functions must not be compromised by allowing critical portions of the program to be performed by employees who have access to the accounts or the computer. Employees should perform various audit functions in areas distinct from their individual duties and responsibilities. Audit findings should be reported directly to the institution's board of directors or to its audit committee. Independent end-user audit coverage can also be provided by external auditors when conducting their annual review.

All facets of end-user computing should be reviewed within an approved audit cycle. The frequency and scope of the audits should be associated directly with the inherent risk in the operation or application function. As such, some activities will be reviewed more frequently than others. The board of directors, or its audit committee, should approve the end-user audit schedule each year. Responsibility for end-user auditing should be clearly assigned by management. Once performed, the audit procedure and findings should be documented, so they may be reviewed and approved by the institution's board of directors. Completed workpapers provide accountability for the audit function and permit the external auditor and supervisory authorities to review its scope and adequacy.

The scope and frequency of end-user computing audits should be determined by analyzing risks associated with end-user computing networks and other forms of distributed processing. Audit and control procedures should be based on management's understanding of those risks. Procedures and responsibilities to manage these risks should be incorporated into an overall corporate information security policy. In performing an audit of an institution's end-user computing system, an auditor should:

- Check for an adequate end-user computing policy.
- Determine if a department or person has been designated to support end-user computing installations.
- Ensure that adequate policies and procedures are used to evaluate, select, and purchase hardware and software.
- Identify the personnel who have functional responsibilities for control and security.

- Determine the number of PC/LAN's and identify their exact location in the networks and the flow of data between them.

- Review the guidelines and procedures established for auditing end-user operations, information systems applications, and user department controls.

- Verify that PC/LAN terminals are in areas that are physically secure during and after normal business hours.

- Ensure that security policies, procedures, and standards have been written.

- Verify that all PC/LAN terminal usage and transaction processing can be identified with a specific person and workstation.

- Determine if risk assessments for all computer applications and programs have been completed.

- Check for established data backup and recovery procedures and compliance with them.

- Assess the procedures for adequate on-site and off-site storage of backup data and programs.

- Assess the level of user training.

- Determine how access to terminals is controlled.

- Verify data integrity.

- Review controls on using and modifying application software.

- Assess downloading/uploading capabilities.

- Verify that the dedicated file server is in a secured area with limited access.

- Determine that plans exist that reflect how PC/LAN's structure and components will be modified if changes occur in the size of the work group or its geographic location.

- Determine if someone has been identified as the PC/LAN administrator, and whether that person understands his/her responsibilities.

- Verify the access controls to ensure unauthorized access is prevented.

- Identify the person responsible for following up on workstation security violations.

- Review report balancing and employee accounts.

- Check the accuracy of master file information and interest and service charge calculations.

- Perform direct verifications of loan and deposit accounts, mainly by the computer if the application software includes a direct verification program or if audit software is available.

- Review the disaster recovery and contingency plans.

- Verify that the disaster recovery and contingency plans are tested and documented at least annually.

- Verify that confidential data is protected when stored on disk and transmitted on PC/LAN network.

An end-user audit function must be established. The procedures should be expanded and improved as needed.

EXAMINING THE IS AUDIT FUNCTION

Examiners must review management and internal controls of IS departments to determine if adequate information systems audit coverage exists. Periodic comprehensive review is necessary to identify potential control problems and provide independent assurance of the reliability of data processing output. Major factors to be considered in an audit review are:

- Competence and size of the information systems audit staff.

- Independence of the audit function.

- Scope, thoroughness, and frequency of audit coverage.

- Documentation of audit work, including workpapers, audit reports, and follow-up.

- Coordination with external auditors.

The audit staff must be reasonably equipped to perform in-depth audits of all information system related areas, including user controls. The auditor's formal education, experience, and self-development through continuing education should be reviewed. The auditor's abilities may be discerned further from discussions with them and a review of audit programs, reports, and related workpapers.

It must be confirmed that auditors operate independently of active management and report their findings and recommendations directly to the board of directors or its committee. Auditors must not perform operational functions that may be subject to audit. In addition, the reporting structure should ensure that their objectivity and independence are not compromised by potentially conflicting duties. Audit independence is essential for an effective audit program.

Audit objectives, goals, schedules, and manuals approved by the board of directors should also be reviewed to help assess audit management and the thoroughness of information systems audit procedures. A review of a representative sampling of recent internal and external audit reports should consider the content of the report, its presentation, and whether reports are addressed to appropriate management levels within the organization. Internal information systems audit workpapers should be compared with the appropriate audit procedures to determine that they are being followed. Established follow-up procedures and written responses to selected internal and external audit reports must also be assessed. Follow-up on deficiencies noted in the previous information systems examination must be performed to determine that promised remedial action has been taken.

Deficiencies in the adequacy of the information systems audit staff, independence of the audit function, or completeness of audit coverage must be detailed in the IS Report of Examination (see Chapter 5, IS Examination Ratings and ROE) and communicated to the board of directors.

A review of the audit function should reveal whether any internal or external information systems audit work can be accepted as a partial or complete substitute for regular examination procedures. Acceptance of such recent audit work in lieu of performing some of these same procedures should:

- Reduce the amount of redundancy in the review of information systems functions.
- Ease the burden on data center management and employee time.
- Result in more effective use of examination personnel.

Audits performed by internal or external auditors that meet acceptable standards probably can be substituted for some examination procedures. This cooperation should foster understanding among auditors and regulatory agency personnel and result in better overall coverage.

Information systems audit work must be performed by qualified, independent audit personnel who follow established audit procedures. It should be recent (within the current audit cycle) and germane to existing data processing operations. To justify reliance upon the audit work of others, the audit scope, procedures, and findings should be discussed with the auditor. The audit procedures and workpapers substantiating the adequacy of information systems audit coverage also should be reviewed. Consistent with the scope of the examination if reliance is placed on the information systems audit coverage, the following procedures must be performed:

- Document those work program sections or steps that will not be performed and describe clearly the auditor's findings and conclusions.
- Follow-up on exceptions noted by the auditor.
- Prepare comments for the IS Report of Examination for those exceptions that remain outstanding and significant.
- Note any reliance upon audit procedures in the section of the report describing the scope of the IS examination.

An examiner's detailed review of external audit procedures and workpapers may not always be necessary to comment on the adequacy of information systems audit coverage. However, such reviews may be necessary if external audit coverage is to substitute for any IS examination procedures. If such a review is deemed necessary, the request for appropriate documentation from the outside auditor should be made through the institution under examination. Occasionally, such requests are resisted by external auditors. Under such circumstances, the examiner must use discretion. Section 112 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) requires that independent public accountants for FDIC-insured institutions provide workpapers and procedures to examiners, if requested.

LEGAL REQUIREMENTS – ANNUAL INDEPENDENT AUDITS

Section 112 of the Federal Deposit Insurance Corporation Improvement Act of 1991 (FDICIA) added a new section 36 to the Federal Deposit Insurance Act (FDI Act), the purpose of which is to facilitate early identification of problems in financial management through annual independent audits, more stringent reporting requirements, and internal controls. The requirements are contained in Part 363 of the FDIC Rules and Regulations and apply to all FDIC-insured depository institutions with total assets of $500 million or more at the beginning of its fiscal year.

Each covered insured depository institution must prepare annual financial statements in accordance with generally accepted accounting principles (GAAP) that must be audited by an independent public accountant. As of the end of its fiscal year, the institution should prepare a report that contains a statement of management's responsibilities for preparing its annual financial statements and for establishing and maintaining an adequate internal control structure and procedures for financial reporting and for complying with designated laws and regulations. The institution also must include an assessment by management of the effectiveness of the internal control structure and procedures as of the end of the fiscal year and its compliance with such laws and regulations during the fiscal year. Service organizations should be considered in determining if internal controls are adequate. On-site reviews of service organizations may not be necessary to prepare the reports required by Part 363. The institution's independent public accountant, its management, and audit committee should exercise independent judgment in making the determination.

Each covered FDIC – insured depository institution must engage an independent public accountant to audit and report on its annual financial statement. The scope of the audit must be sufficient to permit the accountant to determine and report whether the financial statements are presented fairly and in accordance with GAAP.
The independent public accountant must examine, attest to, and report separately on, the assertions of management about the institution's internal control structure and about procedures for financial reporting. The attestations must be made according to generally accepted standards for attestation engagements.

Part 363 of the FDIC Rules and Regulations, including Appendix A, Guidelines and Interpretations, is contained in Chapter 24, Laws and Regulations.